PRIVACY REF

MORSE

Operationalizing Emerging US Privacy Laws

Bob Siegel, President, Privacy Ref

Faith Kasparian, Member, Morse

AGENDA

Introductions

The emerging US laws

A principle-based approach

Operationalizing by principle

PRIVACY REF

Our Speakers

Bob Siegel
bob.siegel@privacyref.com
PRIVACY REF

Faith Kasparian
fkasparian@morse.law
MORSE

About Bob

PRIVACY REF

- President and Founder of Privacy Ref
- Recognized as a Fellow of Information Privacy by the International Association of Privacy Professionals (IAPP) with certifications for US Private Sector Privacy Law (CIPP/US), US Government Privacy (CIPP/G), European Law (CIPP/E), Canadian Law (CIPP/C), IT Practices (CIPT), and Privacy Program Management (CIPM).
- Bob is currently an IAPP training faculty member, having trained more than 8,000 professionals
  - He has also been a member of the Association's advisory boards.
- Privacy Ref provides consulting services aimed at helping businesses develop and implement privacy policies, procedures, and technology to address regulations and employ best practices for handling customer data.

PRIVACY REF

About Faith

MORSE

- Faith is the Chair of the Firm's Privacy and Data Security Practice Group and a Certified Information Privacy Professional/United States (CIPP/US). She is a creative, dynamic, and pragmatic problem solver who loves helping clients mitigate business risk and find practical solutions to legal challenges.
- Faith counsels clients on compliance with state, federal and international privacy laws such as CAN-SPAM, COPPA, FCRA, FERPA, GLBA, HIPAA, TCPA, CCPA, and GDPR, and international data transfer mechanisms; negotiating commercial agreements involving privacy and data security; development of privacy policies and information management best practices; advising on incident and breach response; and privacy risk allocation and due diligence in the context of M&A and investment transactions.

PRIVACY REF

Backdrop for Emerging US Privacy Laws

General Data Protection Regulation (EU) 2016/679 – effective May 28, 2018. Game-changing omnibus privacy legislation that expansively reaches businesses outside the EU with substantial fines for non-compliance. Reflects European view of privacy as a *fundamental human right*.

California Consumer Privacy Act (CCPA) - effective January 1, 2020. The most comprehensive US privacy law of general application. Reflects *synthesis* of historically US *property right* view of privacy *as well as* European *fundamental human right* view.

PRIVACY REF

Emerging US Laws

Enacted but not yet effective

- California Privacy Rights Act (CPRA), Effective January 1, 2023 and expansion of CCPA.
- Virginia Consumer Data Protection Act (CDPA), effective January 1, 2023 and narrower in scope than CCPA.

Introduced

- There is pending data privacy legislation in 10 states, including (at the time of preparing these slides) in Alabama, Colorado, Illinois, Massachusetts, Minnesota, New York, and Texas.
- Certain states, such as New York, have multiple bills pending.

PRIVACY REF

Emerging US Laws
Areas of Alignment

Pending and recently-enacted legislation reflect alignment on certain fundamental data protection concepts, including (as examples) with respect to:

- Broad interpretations of "personal information" meaning, at a minimum, anything about an identified or identifiable natural person
- Required transparency about data practices
- Provision of core data subject rights
- Consent meaning an informed, specific, express manifestation of an individual's wishes (not implied by use)
- Some level of service provider oversight

PRIVACY REF

Emerging US Laws
Areas of Divergence

Some of the areas of divergence include:

- The extent to which individuals will have a ***private right of action***
- Scope
    - Will entities handling a minimum amount of data (e.g., 500, 50K, 100K individuals) be within scope or will revenue thresholds put entities within scope regardless of the amount of data handled?
    - Will employee and B2B data be covered?
    - Will nonprofits be exempt?
- When consent is required (*e.g.*, for all purposes; only to the processing of "sensitive" data; for selling or behavioral advertising, etc.)
- The imposition of fiduciary obligations on covered entities, including to place the individual's data protection rights above the entity's own interest

CHALLENGE

Within this rapidly shifting privacy landscape, how can businesses prepare to operationalize compliance?

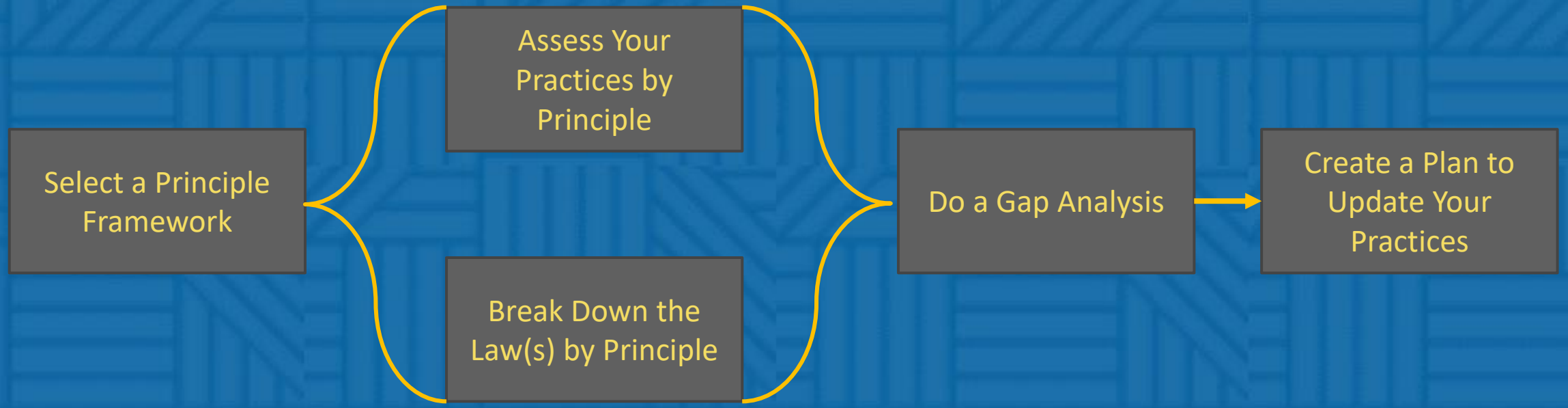
PRIVACY REF

Common requirements

Fair Information Practices	OECD Privacy Principles	Other Considerations
Transparency	Collection Limitation	Data retention
Individual Participation	Data Quality	Data sharing/selling
Purpose Specification	Purpose Specification	Data transfers
Data Minimization	Use Limitation	Enforcement
Security	Security Safeguards	
Accountability and Auditing	Individual Participation	
	Accountability	

PRIVACY REF

Principle-based Approach



PRIVACY REF

Operationalizing by Principle

PRIVACY REF

TRANSPARENCY

Businesses should provide notice about their privacy practices.

- At a high level, most privacy laws require transparency about what information is being collected, the purposes for which it is used, how it is shared with third parties, and the rights individuals have with respect to their information.
- Certain laws will require very specific disclosures and "magic words". As examples:
  - CCPA – chart and granular disclosures including with respect to whether information is being "sold."
  - GDPR – existence of automated decision-making or profiling.
- Certain laws require notices for information collected about all classes of data subjects (*e.g.*, GDPR and CCPA). Certain laws (*e.g.*, Virginia CDPA) exempt employee data from scope.

EXAMPLE: TRANSPARENCY

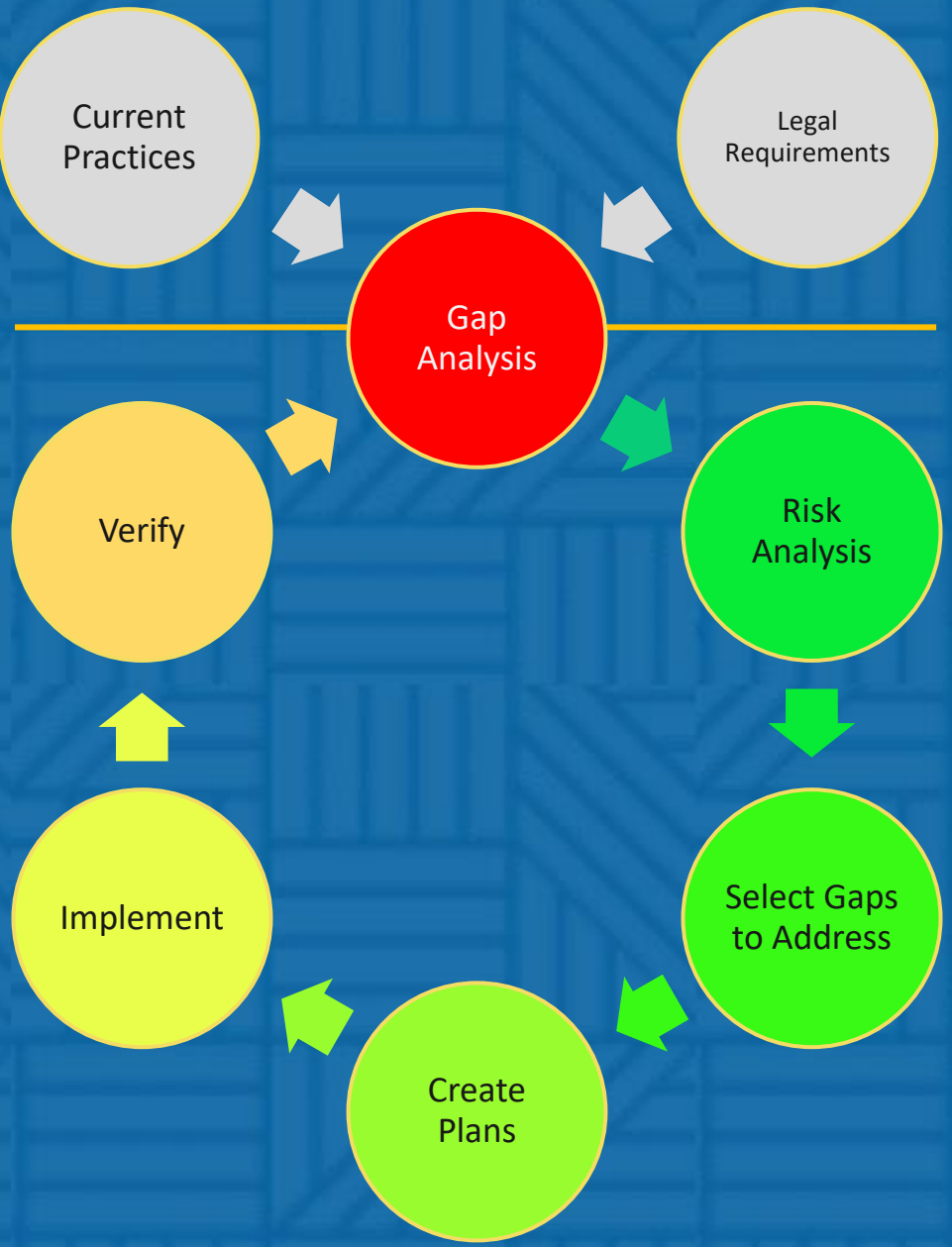
Perform a Gap Analysis

REFERENCE	DESCRIPTION	STATUS: Not Applicable	Not Met	Planned	In Process	Partially Met	Met
Notice Requirements - Generally							
1798.100 (a); 1789.100 (b)	Update or supplement Privacy Notices so that notice is given at the point of or BEFORE collection of consumers' personal information, including the categories of personal information collected, its purpose and how it will be used.					✓	
1798.100 (b)	Update or supplement Privacy Notices indicating that the entity does not collect additional categories of personal information or use personal information collected for additional purposes without a consent notice.						✓
1798.105 (b)	Update or supplement Privacy Notices so that the entity discloses the consumer's right to request deletion of the consumer's personal information, in online privacy policy and in any California specific description of consumer privacy rights (and updates every 12 months)						✓
1798.130 (a) (5):	The entity provides a description of consumer rights regarding the right to request collected personal information and at least one method for submitting requests in its online privacy policy & California-specific privacy rights statements, or, on its website, (updating every 12 months)						✓
1798.130 (a) (5) (B)	The entity discloses a list of the categories of personal information it has collected in preceding 12 months referencing enumerated categories.						✓

PRIVACY REF

EXAMPLE: TRANSPARENCY

Planning Cycle



PRIVACY REF

Operationalizing Steps

Organize legal requirements
- Combine similar requirements
- Determine if there are outliers or requirements for jurisdictional notices

Draft the initial notice
- Determine the structure

Revise the notice for your audience
- Reading level
- Primary language

Enhance the notice
- Layered privacy notice
- Icons/Symbols
- Just-in-time notice
- Videos

Individual Participation

General Requirements

- Businesses should delineate the choices available to individuals and should obtain consent to the collection, use, retention and disclosure of personal information. Consent is considered particularly important for sharing of personal information with other data controllers.
- Businesses should permit individuals to access their personal information for review and update.

Operationalizing Steps

1. Determine your legal basis for processing
2. If using consent, document receipt
   - Capture method, date/time, and meta data of consent. Do the same for revocation of consent.
3. Identify all data subjects' rights you must support
   - Identify affected processes and systems
   - Create functional requirements to support the rights
   - Legal verification of process
   - Train staff
   - Implement

PRIVACY REF

Purpose Specification

General Requirements

- Businesses should collect personal information only for the purposes identified in the respective privacy notice.
- Businesses should share personal information with third parties only for the purposes identified in the respective privacy notice and with the individual's consent.

Operationalizing Steps

1. Construct a data inventory
2. Verify data collected is really needed by each process
3. Perform a gap analysis for the privacy notice and update as appropriate
4. Keep the notice current
   - Privacy by Design
   - Privacy Impact Assessments

Data Minimization

General Requirements

- Businesses use personal information only for the purposes identified in the notice and for which the individual has provided consent.
- Businesses should retain personal information only for as long as needed to fulfill the stated purpose.

Operationalizing Steps

1. Monitor new uses for personal information and new collections
   - Privacy by Design
   - Privacy Impact Assessments
2. Define a Data Retention Policy
3. Create a Records Retention Schedule
4. Monitor compliance

Security

General Requirements

Businesses should implement reasonable administrative, technical and physical safeguards to protect information against unauthorized access, use, disclosure, modification, and destruction. These safeguards should include third-party vendor oversight.

Operational Steps

1. Inform Security (IT and Physical) of requirements.
   - Assess current status through a risk analysis
   - Address gaps as necessary
2. With Security, work with Vendor Management and Procurement to ensure third party compliance
3. Monitor compliance internally and with vendors

Accountability and Auditing

General Requirements

- Businesses must document and communicate their privacy policies and designate (and adequately fund) personnel who will be accountable for these policies.
- And, businesses must monitor compliance with these policies and have procedures to address complaints.

Operational Steps

1. Establish a privacy office budget
   - Personnel
   - Training
   - Tools / Services
2. Create an intranet site
   - Policies, procedures, standards
   - Work aids
3. Create a compliance monitoring program
   - Attestations
   - Assessments
   - Audits

PRIVACY REF

A WORD ABOUT FRAMEWORKS

There are a lot of privacy program frameworks

Select one, core framework

- Must support legal compliance
- Must supply organizational values

Use other frameworks for supporting activities

PRIVACY REF

Connect With Us

Contact us if you have any questions or would like to discuss anything further

PRIVACY REF

www.PrivacyRef.com

info@privacyref.com

888-470-1528

@PrivacyRef

MORSE

www.morse.law

morse@morse.law

781-622-5930

@Morse